Configuring IP Security Services

BayRS Version 13.10
Site Manager Software Version 7.10

Part No. 304111-A Rev 00
November 1998

Bay Networks *Where Information Flows.*™

Bay Networks Where Information Flows.

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. November 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

AN, BN, and Bay Networks are registered trademarks and Advanced Remote Node, ARN, BayRS, BayStack, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xiii
Text Conventions xiv
Acronyms xv
Bay Networks Technical Publications xvi
How to Get Help xvii

Chapter 1
Overview

How IPsec Works 1-1
Network Considerations 1-1
Supported Routers 1-2
Supported WAN Protocols 1-2
IPsec Protection 1-2
IPsec Tunnel Mode 1-3
Security Protocols Overview 1-4
Encapsulating Security Payload 1-4
Authentication Header 1-4
IPsec Services 1-5

Chapter 2
Getting Started with IPsec

Security Gateway 2-2
Security Policies 2-3
Policy Templates 2-3
IPsec Policies 2-4
Criteria Specification 2-4
Action Specification 2-4
Inbound Policies 2-5
Outbound Policies 2-5

Security Policy Database (SPD) 2-6
Security Associations 2-6
Security Associations for Bidirectional Traffic 2-7
Security Parameter Index (SPI) 2-7
Summarizing Security Policies and SAs 2-8
Security Protocols 2-9
IPsec Services 2-10
Confidentiality 2-10
Integrity 2-10
Authentication 2-10
Installing IP Security (IPsec) Software 2-11
Upgrading Software 2-11
Installation Instructions 2-11

Chapter 3
Configuring IPsec

Site Security 3-1
Configuration Security 3-1
Encryption Keys 3-2
Random Number Generator (RNG) 3-2
Node Protection Key (NPK) 3-2
Generating and Using NPKs 3-3
Generating an NPK 3-3
Entering the NPK on the Router 3-4
Entering an NPK and a Seed for Encryption 3-4
Changing NPKs 3-5
Monitoring NPKs 3-6
Enabling IPsec 3-6
Creating Policies 3-7
Criteria Specifications 3-7
Action Specifications 3-7
Policy Considerations 3-8
Creating Security Associations 3-11
Disabling IPsec 3-13

Appendix A
Site Manager Parameters

Node Protection Key Parameter A-1
Enabling IPsec Parameters A-2
IPsec Policy Parameters A-2
Security Association Parameters A-3

Appendix B
Definitions of k Commands

Appendix C
Security Policy and Security Association Examples

Inbound and Outbound Policies C-1
Protect and Unprotect Security Associations (SAs) C-6

Index

Figures

Figure 1-1. IPsec Environment: Unique Security Associations (SAs) Between Routers 1-3
Figure 2-1. IPsec Concepts: Security Gateways, Security Policies, and Security Associations (SAs) 2-2
Figure 2-2. IPsec Security Gateways 2-3
Figure 2-3. Outbound and Inbound Policies 2-6
Figure 2-4. Security Associations for Bidirectional Traffic 2-7
Figure C-1. IPsec Outbound Policies for Routers 1, 2, and 3 ..... C-2
Figure C-2. Single Protect/Unprotect SA Pair C-6
Figure C-3. Multiple Protect/Unprotect SA Pairs C-9

Tables

Table 2-1. Security Policy Specifications 2-8
Table 2-2. Security Association (SA) Configurations 2-8

Preface

This guide describes the Bay Networks® implementation of IP Security and how to configure it on a Bay Networks router.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers* or *Configuring BayStack Remote Access)*.

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.

`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

CBC	cipher block chaining
DES	Data Encryption Standard
ESP	Encapsulated Payload
HMAC	Hashing Message Authentication Code
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICV	integrity check value
IETF	Internet Engineering Task Force
IP	Internet Protocol
IV	initialization vector
MD5	Message Digest 5
MIB	management information base
NPK	node protection key
NVRAM	nonvolatile random access memory

RNG	random number generator
SA	security association
SAD	security associations database
SPD	security policy database
SPI	security parameter index
VPN	virtual private network
WAN	wide area network

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, information about educational services, and the telephone numbers of our global support offices, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

In the United States and Canada, you can dial 800-2LANWAN for assistance.

Chapter 1
Overview

IP Security (IPsec) is the Bay Networks implementation of the Internet Engineering Task Force (IETF) set of standards for security services for communications over public networks. These standards were developed to ensure secure, private communications for the remote access, extranet, and intranet virtual private networks (VPNs) use in enterprise communications.

The Bay Networks implementation of the IETF standard provides network (layer 3) security services for wide area network (WAN) communications on Bay Networks routers.

How IPsec Works

IPsec services are bundled as an Internet Protocol (IP) encryption packet. In this way, any IPsec packet can be delivered over the Internet like an ordinary IP packet to branch offices, corporate partners, or other remote organizations. Unlike an ordinary data packet, the IPsec packet is encrypted. Data traveling across the Internet between IPsec-configured router interfaces can be secure, encrypted, and private.

To configure a router with IPsec, you first configure the router interface as an IP interface. Then you add the IPsec software to the IP interface, creating a *security gateway.*

Network Considerations

To install the IP Security (IPsec) software, the router must be running BayRS Version 13.10 and Site Manager Version 7.10.

Supported Routers

Bay Networks IP technologies are implemented on BayRS router interfaces supporting synchronous communications.

IPsec can provide encryption and authentication services to any serial interface on the following routers:

- BayStack™ Access Node (AN®)
- BayStack Advanced Remote Node™ (ARN™)
- Backbone Node (BN®)
- System 5000™ modules

Supported WAN Protocols

The supported WAN protocols are PPP and frame relay. Bay Networks dial services are also supported. Dial services provide backup and demand services for PPP and frame relay.

IPsec Protection

IPsec protection is implemented by making a router module interface a *security gateway.* The router interface is secured with inbound and outbound security *policies* that filter traffic to and from the router module. The data packets, themselves, are protected with *security associations (SAs)*. For information about security gateways, see “Security Gateway” on page 2-2; for information about inbound and outbound policies, see “IPsec Policies” on page 2-4; and for information about security associations, see “Security Associations” on page 2-6.

Figure 1-1 shows how IPsec can protect data communications within an enterprise and from external hosts.

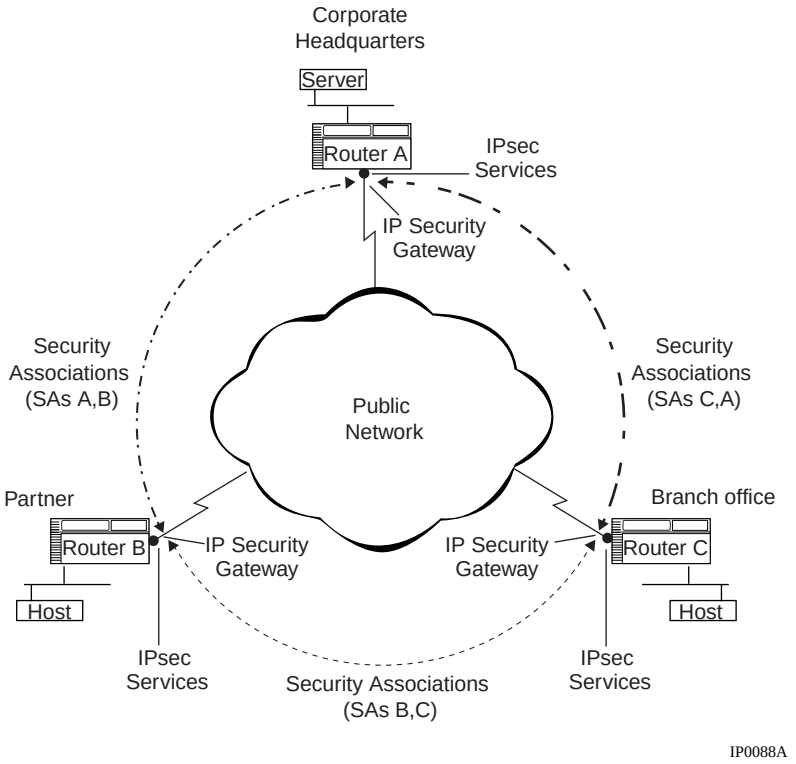

Figure 1-1. IPsec Environment: Unique Security Associations (SAs) Between Routers

IPsec Tunnel Mode

When there is a security gateway at each end of a communication, the security associations between the security gateways are said to be in tunnel mode. All IPsec communications occur in tunnel mode. Tunnel mode is especially effective for isolating and protecting enterprise traffic traveling across a public data network as shown in Figure 1-1.

Security Protocols Overview

IPsec uses two protocols to provide traffic security:

- Encapsulating Security Payload (ESP)
- Authentication Header (AH)

You can use either protocol or both to protect data packets on a VPN.

Encapsulating Security Payload

The ESP protocol provides confidentiality (encryption) services. It can also provide data integrity, data origin authentication, and an anti-replay service. One or more of these security services must be applied whenever ESP is invoked.

ESP uses the Data Encryption Standard (DES) algorithm for encryption and Hashing Message Authentication Code Message Digest 5 (HMAC MD5) transform identifiers. For more information about DES, see “Security Protocols” on page 2-9.

Authentication Header

The AH protocol provides data integrity, data origin authentication, and optional anti-replay services.

The AH protocol uses HMAC MD5 transform identifiers.

IPsec Services

IPsec services include the confidentiality, integrity, and authentication services for data packets traveling between security gateways.

- Confidentiality protects the privacy of communications.
- The integrity service detects modification of data packets.
- Authentication services identify the origin of every data packet.

Within the IPsec framework, additional security services are provided. An access control service ensures authorized use of the network, and an auditing service tracks all actions and events.

IPsec services can be configured on an interface-by-interface basis. Up to 127 inbound and 127 outbound security policies (customized) are supported on each IPsec interface.

For more information about IPsec services, see “IPsec Services” on page 2-10.

Chapter 2
Getting Started with IPsec

IPsec has three key constructs:

- Security gateways
- Security policies
- Security associations (SAs)

In the IPsec context, hosts communicate across an untrusted network through security gateways (routers configured for IPsec interfaces). Security policies determine how the IPsec interfaces handle data packets for the hosts on both ends of a connection. Security associations apply IPsec services to data packets traveling between the security gateways.

Figure 2-1 shows the logical relationship between security policies and security associations.

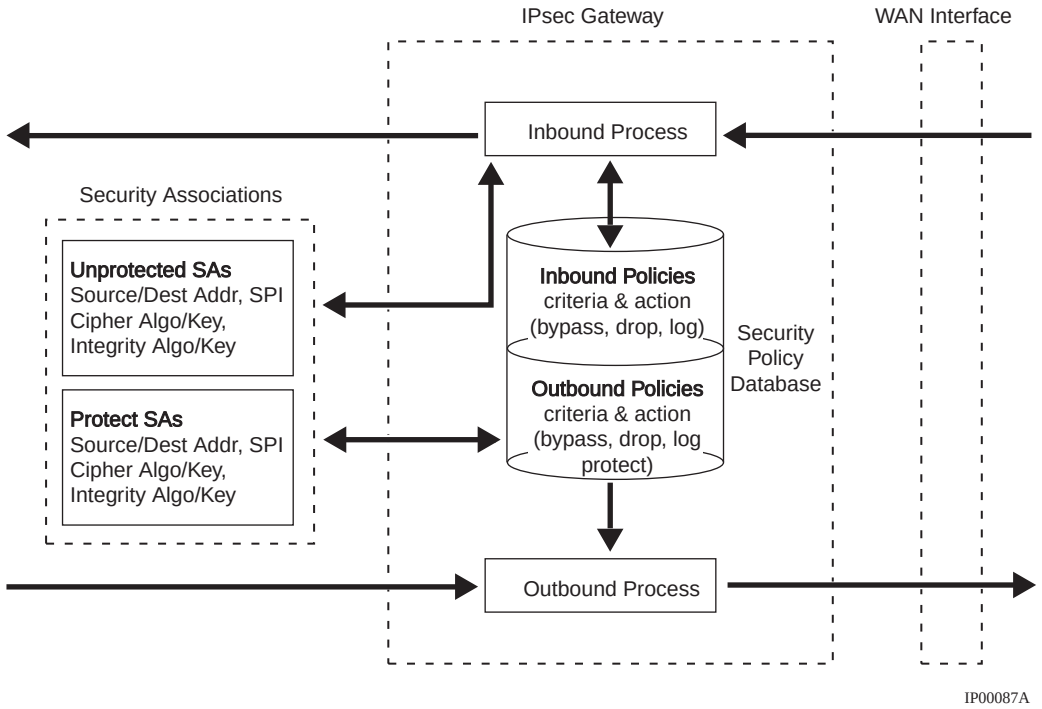

Figure 2-1. IPsec Concepts: Security Gateways, Security Policies, and Security Associations (SAs)

Security Gateway

A Bay Networks router becomes a security gateway when you enable IPsec on a WAN interface.

A security gateway protects one or more security associations between router interfaces configured with IPsec software. A Bay Networks router operating as a security gateway provides IPsec services to its internal hosts and subnetworks.

Hosts or networks on the “external” side of a security gateway are considered “untrusted.” Hosts or subnetworks on the “internal” side of a security gateway are considered “trusted” because they are controlled and securely managed by the same network administration (Figure 2-2).

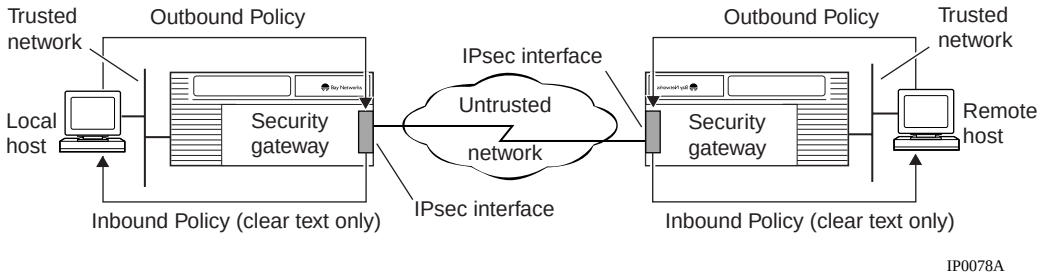

Figure 2-2. IPsec Security Gateways

When you add IPsec services to a security gateway, its internal hosts and subnetworks can communicate with the external hosts that directly operate IPsec services, or with a remote security gateway that provides IPsec services for its set of hosts and subnetworks.

Security Policies

There are two types of IPsec policies: inbound and outbound. An inbound policy is used for data packets arriving at a security gateway, and an outbound policy is used for data packets leaving a security gateway. Each IPsec interface can support up to 127 inbound and 127 outbound security policies (refer to Figure 2-3).

Policy Templates

Every IPsec policy is based on a *policy template*. A policy template is a predefined policy definition that you can use on any IP interface. The template specifies one or more criteria and an action (or none) to apply to incoming or outgoing data packets.

A policy template and every policy based on it must include at least one criterion, for example, an IP source address. A policy template may include one or no action. For example, an outbound policy might specify a protect action. The criterion specification determines whether a data packet matches a particular security policy, and the action specifies how the policy is applied to the packet.

IPsec Policies

When you create an IPsec policy, you control which packets a security gateway protects.

Criteria Specification

IPsec software inspects IP packet headers based on the specified criteria to determine whether a policy applies to a data packet.

You must include at least one of the following criteria, and you may specify all three criteria in an IPsec policy:

- IP source address
- IP destination address
- Protocol

To specify the protocol criterion, you must provide the numeric value assigned to the protocol for use over the Internet. You can specify only a single protocol value for each policy. The protocol number is represented in the 1-byte protocol field in an IP packet header.

To obtain a list of the numeric values assigned to various protocols, see the Internet Assigned Numbers Authority (IANA) Web site at:

http://www.iana.org

The direct path to the list of legal values that you can specify for an IPsec policy protocol criterion is:

http://www.isi.edu/in-notes/iana/assignments/protocol-numbers

Action Specification

A security policy may have one action specification or none. For example, if the IPsec interface is configured with an unprotect SA for an incoming data packet, you do not need an action specification.

The action specifications that you can include in an inbound policy are listed in the next section; action specifications for an outbound policy are listed in “Outbound Policies” on page 2-5.

Inbound Policies

An inbound policy determines how a security gateway processes clear-text data packets received from an untrusted network. Every packet arriving at a security gateway is compared with the criteria to determine whether it matches an IPsec policy for that router. If the incoming packet matches a policy, it can enter the router; if not, it cannot pass through the security gateway.

For an inbound security policy, the action may be:

- Drop
- Bypass
- Log
- No action

Outbound Policies

An outbound policy determines how a security gateway processes data packets for transmission across an untrusted network. You must assign an outbound policy for all unicast traffic leaving an IPsec interface.

For an outbound policy, the action specification may be:

- Drop
- Bypass
- Protect
- Log

Any outbound policy with a protect action specification is mapped to a protect security association (SA). See “Security Associations” on page 2-6 for detailed information about protect and unprotect SAs.

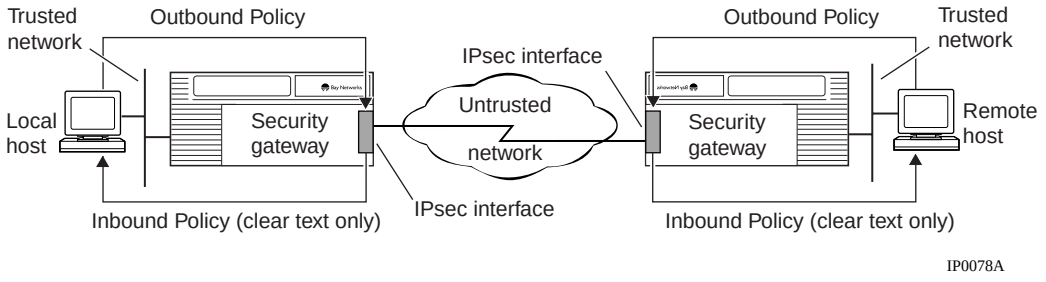

Figure 2-3. Outbound and Inbound Policies

Security Policy Database (SPD)

The criteria (“selectors”) and action specifications used in your inbound and outbound policies are stored in the security policy database (SPD).

IPsec defaults in favor of more security rather than less. If an outbound or inbound packet does not match the criteria of any configured outbound or inbound policy in the SPD, the packet is dropped.

IPsec discards any outbound clear-text data packet unless you explicitly configure a policy to drop, bypass, or protect it.

Security Associations

A security association (SA) is a secure tunnel through which only the hosts that you identify can exchange the protocol data that you specify at the degree of protection that you specify.

A security association is uniquely identified by an IP destination address, security parameter index (SPI), and security protocol identifier (ESP in tunnel mode).

An IPsec policy determines which packets will be handled. A security association (SA) specifies which IPsec security service (for example, confidentiality) IPsec will apply to the packets. You can apply one or more IPsec security services.

Security Associations for Bidirectional Traffic

A security association provides security services to data packets traveling in one direction between secure gateways. To secure the traffic between two security gateways in both directions, you must configure a protect SA for data transmitted from the local IPsec interface and an unprotect SA for data received by the local IPsec interface (Figure 2-4).

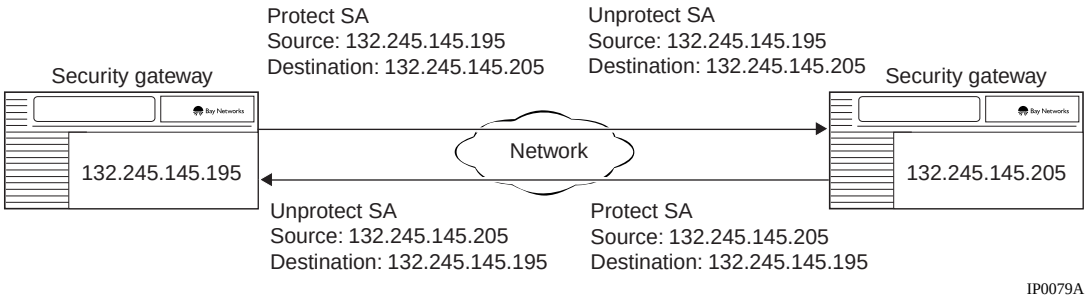

Figure 2-4. Security Associations for Bidirectional Traffic

Security Parameter Index (SPI)

A security parameter index (SPI) is an arbitrary but unique 32-bit value that, when combined with the IP destination address and the numeric value of the security protocol used (ESP), uniquely identifies the SA for a data packet. Although the SPI field is 32-bit, the configuration allows only 16-bit entries.

IPsec discards any incoming ESP packet if the security parameter index (SPI) does not match any SA in the security associations database (SAD).

Summarizing Security Policies and SAs

Table 2-1 and Table 2-2 provide a framework for understanding IPsec policies and security associations (SAs).

In Table 2-1, each row defines the policy specification for the policy named in the first column. For example, the “blue” policy specifies two criteria -- IP source address and IP destination address -- and the “drop” action.

The yellow and green policies specify a protect SA action. You create the SAs for a policy immediately after you specify the policy using them (Table 2-2).

Table 2-1. Security Policy Specifications

Policy Name	Protocol	IP Source Address	IP Destination Address	Action
Blue		IP address	IP address	Drop
Yellow		IP subnet	IP subnet	Protect SA
Green		Range of IP addresses	Range of IP addresses	Protect SA
Black		Any IP address		Bypass

In Table 2-2, the IP source and destination addresses for the SA are those of the tunnel through which the traffic passes. Intermediate routers will protect “protect” SA traffic until it reaches the IP destination address.

Table 2-2. Security Association (SA) Configurations

Security Association		SPI	Cipher			Integrity	
Source Address	Destination Address		Algorithm	Key Length	Key	Algorithm	Key
IP address	IP address	270	DES	40	Hex value	HMAC MD5	Hex value
IP address	IP address	260	DES	50	Hex value	MD5	Hex value

Security Protocols

IPsec uses the following encryption services:

- Data Encryption Standard (DES)
- Message Digest 5 (MD5)

ESP uses the cipher block chaining (CBC) mode of the DES encryption algorithm. CBC is considered the most secure mode of DES. A 56-bit or 40-bit number that you generate, known as a *key*, controls encryption and decryption. Key management is manual.

DES is available in two encryption strengths:

- 56-bit DES keys (recommended)
- 40-bit DES keys

Both sides of an SA must use the same encryption strength. Normally, you should use the stronger 56-bit DES key. However, if you are communicating with a security gateway that is limited to a 40-bit DES key, you must use the 40-bit key.

When ESP protection is used in tunnel mode, an “outer” IP header specifies the IPsec processing destination, and an “inner” IP header specifies the (apparently) ultimate destination for the packet. The security protocol header appears after the outer IP header and before the inner one. Only the tunneled packet is protected, not the outer header.

IPsec Services

IPsec services consist of confidentiality, integrity, and authentication.

Confidentiality

Confidentiality is accomplished by encrypting and decrypting data packets. The Encapsulating Security Payload (ESP) protocol uses the Data Encryption Standard (DES) algorithm in cipher block chaining (CBC) mode to encrypt and decrypt data packets.

You set confidentiality with the cipher algorithm and cipher key parameters. The cipher algorithm and cipher key are specified in the SAs. The algorithm and key must be identical on both ends of an IPsec connection.

Integrity

Integrity determines whether the data has been altered during transit. The ESP protocol ensures that data has not been modified as it passes between the security gateways. The ESP protocol uses the HMAC (RFC 2104) and MD5 (RFC 1321) algorithms.

You set integrity with the integrity algorithm and integrity key parameters. The integrity algorithm and integrity key must be identical on both ends of an IPsec connection.

Authentication

Authentication ensures that data has been transmitted by the authorized source.

Installing IP Security (IPsec) Software

Before you can enable and use IPsec services, you must create an IPsec-capable router image. You create this image during the installation process. The installation instructions that appear on the IP Security (IPsec) software CD are included in this section. To install the IPsec software, you must be running BayRS Version 13.10 and Site Manager Software Version 7.10.

Upgrading Software

If you are upgrading your router software, copy the router image from the upgrade CD to a directory on your hard drive. To modify an existing image, first use the Router Files Manager to transfer the image to a directory on your hard drive.

For instructions on upgrading router software, see *Upgrading Routers to Version 13.xx*. For information about the Image Builder, the Router Files Manager, and booting routers, see *Configuring and Managing Routers with Site Manager.*

Installation Instructions

To install the IP Security (IPsec) software:

1. Insert the IP Security (IPsec) software CD into the CD-ROM drive.
2. Open or create a directory for your router platform (for example, BN).
3. Copy the files *bn.exe* and *capi.exe* to the platform directory.
4. From Site Manager, start the Image Builder (Tools > Image Builder).
5. Open the image in the router platform directory (for example, *bn.exe*). Note that “Available Components” is empty and that “Current Components” lists the executables.
6. Click on Details.

   Under `4003x Baseline Router Software`, select *capi.exe*.
7. Click on Remove.
8. The file *capi.exe* is now listed under Available Components.
9. Choose File > Save to save the image.
10. Exit the Image Builder.

To complete the installation process:

1. Open the Image Builder directory:
   - On a PC, the default directory is *wf\builder.dir\rel<release_number>*
   - On a UNIX platform, the default directory is *~.builder/rel<release_number>*
2. Remove the file *capi.exe* from the Image Builder directory. This file is a 1-byte stub file.
3. Copy the new *capi.exe* file from the router platform directory (for example, BN) to the Image Builder directory.
4. Restart the Image Builder and open the image from which you removed *capi.exe*.
5. Click on Details in the Available Components box.
6. Select *capi.exe* and click on Add.
7. Check the size of the *capi.exe* file.

   If it is less than 1 KB, you have not loaded IPsec software. Repeat this procedure or call the Bay Networks Technical Solutions Center for assistance.
8. Save the modified image that includes IPsec to a new file and exit the Image Builder.
9. Copy this new image to the router and reboot.

Chapter 3
Configuring IPsec

Before you configure IPsec, you need to:

- Install IP Security (IPsec) software (see “Installing IP Security (IPsec) Software” on page 2-11).
- Secure your site.
- Secure your configuration.
- Select an encryption strength.
- Use the Technician Interface secure shell to enter a node protection key (NPK), and then enter the same NPK in Site Manager.

Site Security

To enforce IPsec, carefully restrict unauthorized access to the routers that encrypt data and the workstations that you use to configure IPsec. Keep in mind that the DES and MD5 encryption standards that IPsec uses are public. Your data is secure only if you properly protect the encryption keys. The configuration files that contain these keys include safeguards to prevent unauthorized access.

Configuration Security

Store any files containing encryption keys on diskettes (or other removable media), and keep the media in a secure place. Physically protecting your equipment is always a good strategy and the easiest way to prevent unauthorized access to these files.

Always configure your NPKs locally, not over a network. When you connect a PC or a workstation to a router console port to configure encryption, use a machine that is not connected to any other equipment.

Be sure to also protect the routers on which the NPKs reside.

Encryption Keys

IPsec uses a hierarchy of keys to protect and transmit data:

- Node protection key (NPK) -- encrypts the cipher and integrity keys
- Cipher key -- encrypts data that travels across the network in the ESP payload
- Integrity key -- calculates the integrity check value (ICV), which is used at the data packet destination to detect any unauthorized modification of the data

Caution: The NPK is the most critical key in the hierarchy. If the NPK is compromised, all encrypted data on the router can be compromised.

Random Number Generator (RNG)

The router software uses the secure random number generator (RNG) in Site Manager to generate initialization vectors (IVs) that are used in the ESP DES encryption transformation. These values are statistically random. As its source, the RNG uses a *seed* that you supply from the Technician Interface secure shell. See “Entering an NPK and a Seed for Encryption” on page 3-4.

Node Protection Key (NPK)

The NPK encrypts cipher and integrity keys for MIB storage. Note that it does not encrypt, decrypt, or authenticate data.

The NPK is stored in the router nonvolatile random access memory (NVRAM). Its fingerprint, which is a 128-bit version of the NPK generated by a hash algorithm, is stored in the management information base (MIB). For encryption to occur, the NPK and its fingerprint in the MIB must match.

Create and configure a different NPK for each secure router on your network. The NPK should be different on every router because, if an NPK is compromised, the security gateway for the router is compromised. If the same NPK is used for all secure routers, the entire network could be compromised.

Caution: Be very careful to protect all files where NPKs are stored. You should store your NPKs on removable media (for example, diskettes) and keep the media in a secure location.

Generating and Using NPKs

You create NPKs using the Technician Interface secure shell. You must then enter the same NPKs into the Site Manager NPK parameter for that router. For details, see the note later in this section.

The following steps summarize how an NPK is used. Detailed steps for using NPKs appear later in this chapter (see “Entering an NPK and a Seed for Encryption” on page 3-4).

1. You are responsible for creating NPKs. The NPK value should be a random number (16 hexadecimal digits). Use a unique NPK for each router.
2. Enter an NPK value in the router NVRAM, using the secure shell of the Technician Interface. Do this for each secure router.
3. Enter the same NPK value in the Site Manager IPsec Node Protection Key parameter for the router that you are configuring.

Generating an NPK

To generate an NPK, use a method available at your site to create random 16-digit hexadecimal numbers.

Note: You can use the NPK Key Manager to generate NPKs. The NPK Key Manager is available from the WEP Key Manager. To access it, open the main window in Site Manager and choose Tools > WEP Key Manager > NPK Manager. During IPsec processing, you can manually enter the same NPKs in the Technician Interface. For detailed information, see *Configuring Data Encryption Services*.

Entering the NPK on the Router

You enter the NPK into a router locally, using the console port and the secure shell section of the Technician Interface. A password protects access to the secure shell.

You cannot access the NPK or the password using the MIB or the routine Technician Interface debug commands. Nor can you invoke the secure shell in a Telnet session.

Caution: Never use a terminal server to enter the NPK. Instead, use a laptop computer that you can attach directly to the router. Protect the file containing NPKs on the laptop.

Entering an NPK and a Seed for Encryption

Before you can add IPsec to a router, you must enter an NPK and create a *seed* for encryption using the Technician Interface secure shell. IPsec uses the NPK to encrypt and decrypt the cipher and integrity keys, and it uses the seed specified with the **kseed** command to encrypt data.

To enter an NPK and a seed for encryption:

1. If you do not have a password for the Technician Interface secure shell, you must create one. Enter **kpassword** <*password*>.

   For *password*, enter an alphanumeric value up to 16 characters.

2. At the Technician Interface prompt, type **ksession** to enter the Technician Interface secure shell. (If you issue the **ksession** command before setting a password, you will be prompted to do so. Use **kpassword** and step 1.)

3. Enter the **kseed** command. The secure shell prompts you for a random seed value.

   Type a random set of keystrokes. The secure shell informs you when you have entered the required number of keystrokes.

4. Type **kset npk 0x**<*NPK_value*>.

   Type **0x** and the 16-digit hexadecimal NPK value that you assigned to the router that you are configuring. For more information, see “Generating and Using NPKs” on page 3-3.

The **kset npk** command stores your *NPK_value* in the router NVRAM, and it calculates a hash of this value that it stores in the router MIB.

5. Enter the **save config** <*config_file_name*> command. You cannot exit the secure shell without saving the configuration. This is necessary so that upon rebooting the router with the saved configuration file, the hash of the NPK in the MIB corresponds with the NPK in NVRAM.
6. Enter **kexit** to exit the secure shell.

Changing NPKs

To maintain security, periodically change the NPKs entered into the routers.

To change an NPK, enter the **kset NPK** command, using the steps you used to create the original NPK (see “Entering an NPK and a Seed for Encryption” on page 3-4).

The new NPK overwrites the original, and IPsec uses the new NPK value.

To change the NPK value used by the MIB:

1. At the Technician Interface prompt, enter **ksession**.

   This command allows you to enter the secure shell. You are prompted for your password.
2. Enter your password.

   The prompt changes to: `SSHELL`.
3. Enter **ktranslate** *<old_NPK_value>*.

   The MIB now has the same NPK as the router.
4. Save the configuration file.

Monitoring NPKs

If the NPK on a router does not match the NPK in the MIB, IPsec services do not work. This type of situation usually occurs when you change a CPU board in a router slot and the slot now lacks the current NPK, or you revert to an older configuration that is protected by an older NPK.

View the router log to make sure that the NPK for each slot matches the NPK value in the MIB. If not, using the secure shell, change either the router NPK value or the MIB NPK value. For more information about changing NPKs, see "Changing NPKs" on page 3-5.

To view the router log events specific to an NPK in the Technician Interface, enter:

log -ffwldt -eKEYMGR

Enabling IPsec

To enable IPsec, configure an IP interface using the Configuration Manager. Then add IPsec services to that interface to create a security gateway. Use the following steps.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the WAN connector on which you want to configure an IPsec interface.	The Add Circuit window opens.
2. Click on **OK**.	The WAN Protocols window opens.
3. Choose a WAN protocol (PPP or frame relay).	The Select Protocols window opens.
4. Choose **IP** and **IPSEC**.	The IP Configuration window opens.
5. Set the following parameters: • **IP Address** • **Subnetwork Mask** Click on **Help** or see *Configuring IP Services*.	
6. Click on **OK**.	The IPsec Configuration for Interface window opens.

When you use Site Manager to configure IPsec on an interface for the first time, configure the menu items displayed in the IPsec Configuration for Interface window in sequence, starting with the top item, Outbound Policies. You must set an outbound policy for an IP interface before you can link a security association (SA) to it.

Creating Policies

You create inbound and outbound policies for an IP interface by using a policy template. A policy template is a policy definition that you create. You can use a policy template on any IP interface.

Each template contains a complete policy specification (criteria, range, and action) for the interface. This means that each policy itself is completely specified by the template. You can modify an individual policy to fit the needs of a specific interface, as long as the values in the policy comply with the policy template specifications. For example, an IP source address value must be in the range specified in the policy template.

Criteria Specifications

The criteria determine the portion of a packet header (IP source address, IP destination address, protocol number) that is examined by IPsec. For each criterion, you must specify a range of values. The range represents the actual criteria values (IP addresses that are compared to the address of a packet).

Action Specifications

The action specification in a policy controls how a packet that matches the specified criteria (and criteria range) is processed. You decide how you want packets to be processed and apply a policy to implement your decision.

With IPsec, a packet can be processed in one of three ways:

- The packet can be dropped.
- The packet can be transmitted or received without alteration.
- The packet can be protected. In this case, a security association (SA) is linked to the policy.

The corresponding policy actions are:

- Drop
- Bypass
- Protect
- Log (a message will be written to the router log)

The first three actions are mutually exclusive. You can specify a logging action for any of the other three actions. Note that if an incoming packet that does not match any configured policy arrives at an IPsec interface, it is dropped by default.

Policy Considerations

When you configure a WAN interface with IPsec, all inbound and outbound traffic on that interface is processed by IPsec, including traffic being forwarded.

For unicast traffic containing routing or control information, consider configuring policies that allow such traffic to bypass IPsec. For example, to allow ICMP traffic (such as “ping” or “destination unreachable” messages) to bypass IPsec processing, configure the first policy for the interface with the protocol criterion set to number 1 (ICMP) and the action specification set to bypass.

If a data packet matches the criteria for more than one policy, the first matching policy is used.

To create an outbound policy template and policy, complete the following tasks:

Site Manager Procedure		
	You do this	**System responds**
Policy Template	1. In the IPsec Configuration for Interface window, click on **Outbound Policies**.	The IPsec Outbound Policies window opens.
	2. Click on **Template**.	The IPsec Policy Template Management window opens.
	3. Click on **Create**.	The Create IPsec Template window opens.
	4. Enter a name in the **Policy Name** field. Click on **Help**, or see the parameter description on page A-3.	
	5. Use the **Criteria** menu to specify the applicable range for the IP source addresses, IP destination addresses, and protocol criteria.	
	6. Use the **Action** menu to add the action that you want applied to traffic with the criteria that you just defined.	
	7. Click on **OK**.	You return to the IPsec Policy Template Management window.
	8. Click on **Done**.	You return to the IPsec Outbound Policies window.
	Note: If you selected **Protect** from the **Action** menu for this policy, Site Manager displays an inquiry window that asks whether you want to immediately create a security association to link with this policy.	

(continued)

Site Manager Procedure *(continued)*		
	You do this	**System responds**
Policy	9. Click on **Add Policy**.	The Create Outbound Policy window opens.
	10. Enter the policy name in the **Policy Name** field. Click on **Help** or see the parameter description on page A-3.	
	11. Select a template on which to base this policy.	
	12. Click on **OK**.	You return to the IPsec Outbound Policies window.
	Note: If you choose, see the instructions for configuring an SA in "Creating Security Associations." If you do not want to configure an SA at this time, continue this procedure.	
	13. Click on **Done**.	You return to the IPsec Configuration for Interface window.

Creating Security Associations

Security associations enable you to provide bidirectional protection for data packets traveling between two routers. However, each SA establishes security for data passing in a single direction.

An SA exists for any IPsec policy supported by a security gateway. Each policy includes security information such as algorithms, or keys, that must be tracked. To protect (encrypt or authenticate) data packets leaving the local IP interface, create a protect SA and link it to an outbound policy.

To decrypt or authenticate incoming packets at the local IP interface, create an unprotect SA. (The unprotect SA does not need to be linked to a policy.) Then, do the same for the IP interface on the remote router.

The cipher and integrity algorithms and keys that you specify in SAs must be identical on both ends of a connection. You must select either the cipher or the integrity service or both within the protect and unprotect SA parameters. For example, the cipher key in a protect SA on the local IP interface must match the cipher key in the unprotect SA on the remote router IP interface.

Note: SAs must be configured to encrypt, authenticate, or both. Site Manager does not allow you to create an SA if both the Cipher Algorithm and the Integrity Algorithm parameters are set to None.

To create a protect SA, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the IPsec Configuration for Interface window, click on **Protect SA**.	The Protect SA for Interface window opens.
2. Click on **Add**.	The parameters in the Protect SA for Interface window become active.
3. Set the following parameters: • **SA Source IP Address** • **SA Destination IP Address** • **Security Parameter Index** • **Cipher Algorithm** • **Cipher Key Length** • **Cipher Key** • **Integrity Algorithm** • **Integrity Key** Click on **Help**, or see the parameter descriptions beginning on page A-3.	
4. Click on **OK**.	Either the Outbound Policy window or the IPsec Configuration for Interface window opens. Use the Outbound Policy window and the following steps to link the protect SA to an outbound policy.
5. In the Outbound Policy window, select the policy to which you want to apply an SA.	
6. Click on **SA**.	The list of SAs appears.
7. Click on the **SA** to apply to this policy.	
8. Click on **OK**.	

Disabling IPsec

To disable IPsec on all router interfaces configured for it, complete the following tasks. (You cannot disable IPsec on an individual interface.)

Site Manager Path	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IP Security**.	The IP Security menu opens.
4. Choose **Globals**.	The Edit IP Security Global Parameters window opens.
5. Set the **IP Security Enable** parameter to **Disable**.	
6. Click on **Done**.	You return to the Configuration Manager window.

Appendix A
Site Manager Parameters

This appendix describes the Site Manager parameters for:

- Creating a node protection key (NPK)
- Enabling IPsec
- Configuring IPsec policies
- Configuring IPsec security associations

Node Protection Key Parameter

Parameter:	**Node Protection Key**
Path:	Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)
Default:	None
Options:	An 8-byte value
Function:	Used as a cryptographic key for protecting sensitive MIB objects. The NPK value is stored in nonvolatile random access memory (NVRAM). The IPsec software performs a hash of the NPK value, which it places in a special MIB attribute. The NPK value stored in NVRAM is unique to the router. It is used to encrypt the cipher and integrity keys before they are stored in the router MIB.
Instructions:	Enter a 16-digit hexadecimal value. (Enter the prefix 0x before the digits.)
MIB Object ID:	NA

Enabling IPsec Parameters

Parameter: **IP Security Enable**

Path: Configuration Manager > Protocols > IP > IP Security > Globals

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPsec on a router. If this parameter is set to Disable, you cannot implement IPsec.

Instructions: To implement IP security on a router, set this parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.26.1.2

Parameter: **Maximum SPI**

Path: Configuration Manager > Protocols > IP > IP Security > Globals

Default: 384

Options: 256 through 65535

Function: Specifies the maximum acceptable security parameter index (SPI) value for configured security associations (SAs).

Instructions: Enter a value that is unique for the security associations (SAs) defined for this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.26.1.5

IPsec Policy Parameters

Parameter: **Policy Enable**

Path: Configuration Manager > Protocols > IP > IP Security > Outbound Policies

Default: Enable

Options: Enable | Disable

Function: Determines whether the named policy will be used on the IP interface.

Instructions: Set this parameter to Enable to activate the named policy on the IP interface.

MIB Object ID: NA

Parameter: **Policy Name**

Path: Configuration Manager > Protocols > IP > IP Security > Outbound Policies

Default: None

Options: Any valid name

Function: Specifies the name of the policy to be created using the IPsec policy template.

Instructions: Enter a name to identify any policy you create using the IPsec policy template.

MIB Object ID: NA

Security Association Parameters

Parameter: **SA IP Source Address**

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: None

Options: Any valid IP address

Function: Specifies the IP address of the source interface for this unidirectional security association (SA).

Instructions: For a protect SA, enter the IP address of the local IPsec interface. For an unprotect SA, enter the IP address of the remote IPsec interface.

MIB Object ID: NA

Parameter: **SA IP Destination Address**

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: None

Options: Any valid IP address

Function: Specifies the IP address of the destination interface for this unidirectional security association (SA).

Instructions: For a protect SA, enter the IP address of the remote IPsec interface. For an unprotect SA, enter the IP address of the local IPsec interface.

MIB Object ID: NA

Parameter: Security Parameter Index

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: 256

Options: 256 through 65535

Function: The security parameter index (SPI) is an arbitrary 32-bit value that, when combined with the destination IP address and the numeric value of the security protocol being used (ESP), identifies the security association (SA) for the data packet.

Instructions: Enter a value from 256 through 65535.

MIB Object ID: NA

Parameter: Cipher Algorithm

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: DES CBC

Options: None | DES CBC

Function: Identifies the cipher algorithm for this security association (SA).

Instructions: To implement the cipher (or confidential/encrypted) level of security, select the Data Encryption Standard (DES) algorithm. If you select None, this level of security will not be applied to data packets processed according to this security association (SA); that is, the data packets will not be encrypted.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.26.5.1.6

Parameter: Cipher Key Length

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: DES56

Options: DES40 | DES56

Function: Identifies the cipher key length (strength) for this security association (SA).

Instructions: Select a cipher key length of either 40 or 56 bits. The longer key length (strength) provides greater security.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.26.5.1.8

Parameter: Cipher Key

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: None

Options: Any valid 8-byte value

Function: Specifies the key for a security association cipher algorithm. This key value must match on both sides of an SA to enable the encryption and decryption of data packets according to the Data Encryption Standard (DES) algorithm.

Instructions: Enter a 16-digit (8-byte) hexadecimal value. (Enter the prefix 0x before the 16 digits.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.26.5.1.7

Parameter: Integrity Algorithm

Path: Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)

Default: None

Options: None | HMAC MD5

Function: Enables implementation of the HMAC MD5 algorithm, which determines whether a data packet was changed between the source and destination.

Instructions: To implement the security integrity level, select the HMAC MD5 algorithm. If you select None, this level of security will not be applied to data packets processed according to this security association (SA); that is, IP security cannot determine whether a data packet was changed between the source and destination.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.26.5.1.9

Parameter:	**Integrity Key**
Path:	Configuration Manager > Protocols > IP > IP Security > Security Associations (SAs)
Default:	None
Options:	Any valid 16-byte value
Function:	Specifies the key for a security association (SA) integrity algorithm. This key value must match on both sides of an SA to enable the integrity algorithm to determine whether a data packet was changed between the source and destination.
Instructions:	To establish the integrity level of IP security, enter a 32-digit hexadecimal value. (Enter the prefix 0x before the 32 digits.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.26.5.1.10

Appendix B
Definitions of k Commands

This appendix contains definitions of the “k” commands that you use to work in the Technician Interface secure shell.

Command	System Response
kexit	Exits the secure shell.
kpassword	Changes the password of the secure shell.
kseed	Initializes the cryptographic random number generator while in the secure shell.
ksession	Initiates a secure shell session.
kset *<subcommand>* [*<flags>*]	Sets parameter values in the secure shell. Example: **kset npk** *<value>* sets the router node protection key. Also sets protected IPsec MIB objects (keys). The **kset** command encrypts the value specified using the NPK, and writes the encrypted value to the MIB. Example: **kset ipsec wfIpsecEspSaEntry.wfIpsecEspSaManualCipherKey .100.1.1.1.100.1.1.2.256 0x1234567890abcdef**
ktranslate *<old_NPK>*	Translates a configuration from an old node protection key (NPK) value to the current NPK value. Example: **ktranslate** *<old_npk>*

Appendix C
Security Policy and Security Association Examples

This appendix provides examples of outbound and inbound policies and protect and unprotect security associations.

Inbound and Outbound Policies

All unicast traffic must be defined by a security policy. Traffic traveling from a security gateway is defined by an outbound policy. Traffic traveling to a secure gateway is defined by an inbound policy. Inbound protected traffic that is associated with an unprotect SA configured on the interface does not require a policy.

As you review the security policy examples in this section, refer to Figure C-1.

All of the routers have OSPF interfaces configured for type NBMA transmit unicast frames. An outbound and an inbound bypass policy protect all unicast traffic for the specified router subnetworks.

Security policy examples 1 and 2 show how to configure outbound policies to protect all unicast traffic between router (RTR) 1 and router 2; examples 3 and 4 show how to configure outbound policies to protect all unicast traffic between router 2 and router 3; and examples 5, 6, and 7 show how to configure outbound policies to protect all traffic between router 1 and router 3. A bypass inbound policy is in effect for all incoming traffic to the routers so that no SAs are required.

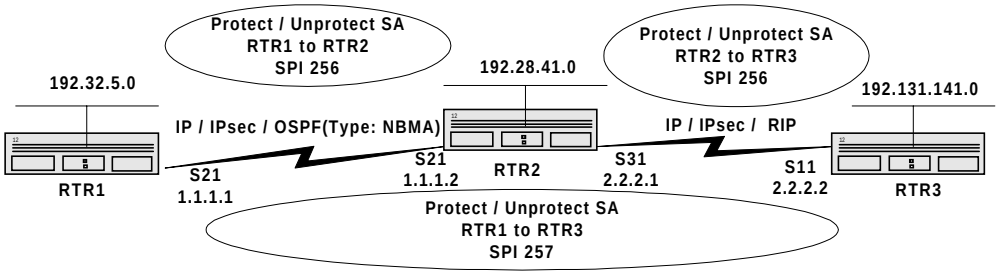

Figure C-1. IPsec Outbound Policies for Routers 1, 2, and 3

Example 1: Required Policies on RTR 1 to Protect Data Between RTR 1 Subnet 192.32.5.0 and RTR 2 Subnet 192.28.41.0

Router RTR 1	**Interface S21**	
Policy	Outbound	
Action	Protect	
Criteria	IP source address range:	192.32.5.0 - 192.32.5.255
	IP destination address range:	192.28.41.0 - 192.28.41.255
SA	SRC: 1.1.1.1 DST: 1.1.1.2 SPI 256	

RTR1 Interface S21		
Security Policy	Outbound	Inbound
Action	Bypass	Bypass
Criteria	Protocol 89 (OSPFIGP)	Protocol 89 (OSPFIGP)

Example 2: Required Policies on RTR 2 to Protect Data Between RTR 1 Subnet 192.32.5.0 and RTR 2 Subnet 192.28.41.0

Router RTR 2	**Interface S21**	
Policy	Outbound	
Action	Protect	
Criteria	IP source address range:	192.28.41.0 - 192.28.41.255
	IP destination address range:	192.32.5.0 - 192.32.5.255
SA	SRC: 1.1.1.2 DST: 1.1.1.1 SPI 256	

RTR2 Interface S21		
Security Policy	Outbound	Inbound
Action	Bypass	Bypass
Criteria	Protocol 89 (OSPFIGP)	Protocol 89 (OSPFIGP)

Example 3: Required Policies on RTR 2 to Protect Data Between RTR 2 Subnet 192.28.41.0 and RTR 3 Subnet 192.131.141.0

Router RTR 2	**Interface S31**	
Policy	Outbound	
Action	Protect	
Criteria	IP source address range:	192.28.41.0 - 192.28.41.255
	IP destination address range:	192.131.141.0 - 192.131.141.255
SA	SRC: 2.2.2.1 DST: 2.2.2.2 SPI 256	

Example 4: Required Outbound Policies on RTR 3 to Protect Data Between RTR 2 Subnet 192.28.41.0 and RTR 3 Subnet 192.131.141.0

Router RTR 3	**Interface S11**	
Policy	Outbound	
Action	Protect	
Criteria	IP source address range:	192.131.141.0 - 192.131.141.255
	IP destination address range:	192.28.41.0 - 192.28.41.255
SA	SRC: 2.2.2.2 DST: 2.2.2.1 SPI 256	

Example 5: Required Outbound Policies on RTR 1 to Protect Data Between RTR 1 Subnet 192.32.5.0 and RTR 3 Subnet 192.131.141.0

Router RTR 1	**Interface S21**	
Policy	Outbound	
Action	Protect	
Criteria	IP source address range:	192.32.5.0 - 192.32.5.255
	IP destination address range:	192.131.141.0 - 192.131.141.255
SA	SRC: 1.1.1.1 DST: 2.2.2.2 SPI 257	

RTR2 Interface S21		
Security Policy	Outbound	Inbound
Action	Bypass	Bypass
Criteria	Protocol 89 (OSPFIGP)	Protocol 89 (OSPFIGP)

Example 6: Required Policies on RTR 2 to Allow ESP Traffic to Pass Through and OSPF to Exchange Routing Updates Between RTR 1 and RTR 2

RTR2 Interface S21		
Security Policy	Outbound	Inbound
Action	Bypass	Bypass
Criteria	Protocol 89 (OSPFIGP)	Protocol 89 (OSPFIGP)
Security Policy	Outbound	Inbound
Action	Bypass	Bypass
Criteria	Protocol 50 (ESP)	Protocol 50 (ESP)

RTR2 Interface S31		
Security Policy	Outbound	Inbound
Action	Bypass	Bypass
Criteria	Protocol 50 (ESP)	Protocol 50 (ESP)

Example 7: Required Policies on RTR 3 to Protect Data Between RTR 3 Subnet 192.131.141.0 and RTR 1 192.32.5.0

Router RTR 3	**Interface S11**	
Policy	Outbound	
Action	Protect	
Criteria	IP source address range:	192.131.141.0 - 192.131.141.255
	IP destination address range:	192.32.5.0 - 192.32.5.255
SA	SRC: 2.2.2.2 DST:1.1.1.1 SPI 257	

Protect and Unprotect Security Associations (SAs)

Security associations (SAs) specify which IPsec services are applied to the data packets traveling between the security gateways. An individual SA protects data traveling in one direction. A protect SA is used to apply IPsec services to outbound traffic; an unprotect SA is used to decrypt and/or authenticate incoming data packets.

The examples in this section show how to configure both protect and unprotect SAs.

For SA examples 1 and 2, refer to Figure C-2; for SA example 3, refer to Figure C-3.

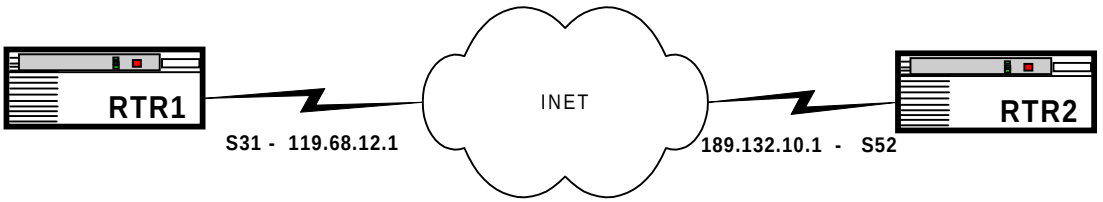

Figure C-2. Single Protect/Unprotect SA Pair

SA Example 1: Configuring a Single Protect/Unprotect SA Pair

In this example, a single protect/unprotect SA pair is configured using DES encryption. Both ends of the SA pair use the same cipher algorithm, cipher key, and integrity key (see Figure C-2).

RTR 1 Protect SA		RTR 2 Unprotect SA
IP source address	119.68.12.1	119.68.12.1
IP destination address	189.132.10.1	189.132.10.1
Security parameter index (SPI)	256	256
Cipher key length	DES56	DES56
Cipher key	0x0101230405060708	0x0101230405060708
Integrity algorithm	HMAC MD5	HMAC MD5
Integrity key	0x010123040506070890a0 b0c0d0e0f11	0x010123040506070890a0 b0c0d0e0f11

	RTR 1 Unprotect SA	RTR 2 Protect SA
IP source address	189.132.10.1	189.132.10.1
IP destination address	119.68.12.1	119.68.12.1
Security parameter index (SPI)	256	256
Cipher key length	DES56	DES56
Cipher key	0x0101230405060708	0x0101230405060708
Integrity algorithm	HMAC MD5	HMAC MD5
Integrity key	0x010123040506070890a0 b0c0d0e0f11	0x010123040506070890a0 b0c0d0e0f11

SA Example 2: Configuring Two Protect/Unprotect SA Pairs

In this example, two protect/unprotect SA pairs are configured using DES encryption. Both ends of the SA pair use the same cipher algorithm and key. The integrity algorithm is set to none (refer to Figure C-2).

	RTR 1 Protect SA	RTR 2 Unprotect SA
IP source address	119.68.12.1	119.68.12.1
IP destination address	189.132.10.1	189.132.10.1
Security parameter index (SPI)	256	256
Cipher key length	DES56	DES56
Cipher key	0x0101230405060708	0x0101230405060708
Integrity algorithm	None	None
Integrity key	None	None

	RTR 1 Unprotect SA	RTR 2 Protect SA
IP source address	189.132.10.1	189.132.10.1
IP destination address	119.68.12.1	119.68.12.1
Security parameter index (SPI)	257	257
Cipher key length	DES56	DES56
Cipher key	0x0101230405060708	0x0101230405060708
Integrity algorithm	None	None
Integrity key	None	None

SA Example 3: Configuring Multiple Protect/Unprotect SA Pairs

In this example, multiple protect/unprotect SA pairs are configured between RTR 1 and RTR 2, RTR 3, and RTR 4.

- The SA pair between RTR 1 and RTR 2 uses DES56 and HMAC MD5.
- The SA pair between RTR 1 and RTR 3 uses only HMAC MD5.
- The SA pair between RTR 1 and RTR 4 uses only DES56.

As you review the tables in this example, refer to Figure C-3.

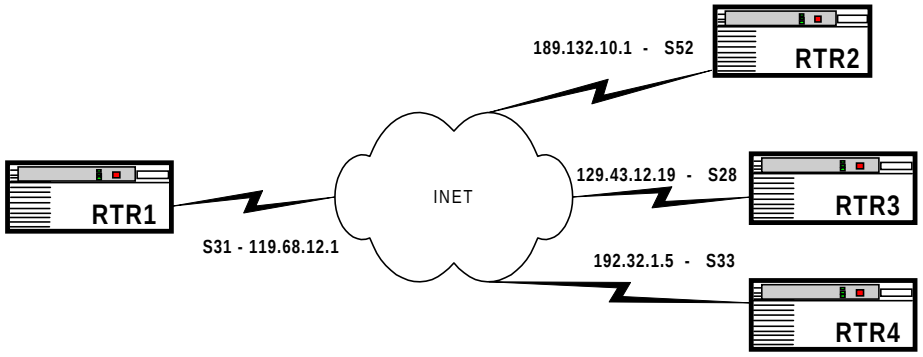

Figure C-3. Multiple Protect/Unprotect SA Pairs

The following two tables show the settings for the protect/unprotect SA pairs between RTR 1 and RTR 2 (refer to Figure C-3).

	RTR 1 Protect SA	RTR 2 Unprotect SA
IP source address	119.68.12.1	119.68.12.1
IP destination address	189.132.10.1	189.132.10.1
Security parameter index (SPI)	257	257
Cipher key length	DES56	DES56
Cipher key	0x0101230405060708	0x0101230405060708
Integrity algorithm	HMAC MD5	HMAC MD5
Integrity key	0x010123040506070890a0 b0c0d0e0f11	0x010123040506070890a0 b0c0d0e0f11

	RTR 1 Unprotect SA	RTR 2 Protect SA
IP source address	189.132.10.1	189.132.10.1
IP destination address	119.68.12.1	119.68.12.1
Security parameter index (SPI)	256	256
Cipher key length	DES56	DES56
Cipher key	0x0101230405060708	0x0101230405060708
Integrity algorithm	HMAC MD5	HMAC MD5
Integrity key	0x010123040506070890a0 b0c0d0e0f11	0x010123040506070890a0 b0c0d0e0f11

The next two tables show the settings for the protect/unprotect SA pairs between RTR 1 and RTR 3 (refer to Figure C-3).

	RTR 1 Protect SA	RTR 3 Unprotect SA
IP source address	119.68.12.1	119.68.12.1
IP destination address	129.43.12.19	129.43.12.19
Security parameter index (SPI)	256	256
Cipher key length	DES56	DES56
Cipher key	0xFADE050403020100	0xFADE050403020100
Integrity algorithm	None	None
Integrity key	None	None

	RTR 1 Unprotect SA	RTR 3 Protect SA
IP source address	129.43.12.19	129.43.12.19
IP destination address	119.68.12.1	119.68.12.1
Security parameter index (SPI)	257	257
Cipher key length	DES56	DES56
Cipher key	0xFADE050403020100	0xFADE050403020100
Integrity algorithm	None	None
Integrity key	None	None

The final two tables show the settings for the protect/unprotect SA pairs between RTR 1 and RTR 4 (refer to Figure C-3).

	RTR 1 Protect SA	RTR 4 Unprotect SA
IP source address	119.68.12.1	119.68.12.1
IP destination address	192.32.1.5	192.32.1.5
Security parameter index (SPI)	256	256
Cipher key length	None	None
Cipher key	None	None
Integrity algorithm	HMAC MD5	HMAC MD5
Integrity key	0x090a0bbb0c0d0e0f11011 02030405060708	0x090a0bbb0c0d0e0f11011 02030405060708

	RTR 1 Unprotect SA	RTR 4 Protect SA
IP source address	119.68.12.1	119.68.12.1
IP destination address	192.32.1.5	192.32.1.5
Security parameter index (SPI)	258	258
Cipher key length	None	None
Cipher key	None	None
Integrity algorithm	HMAC MD5	HMAC MD5
Integrity key	0x090a0bbb0c0d0e0f11011 02030405060708	0x090a0bbb0c0d0e0f11011 02030405060708

Index

Numbers

40-bit DES key, 2-9
56-bit DES key, 2-9

A

acronyms, xv
AH, 1-4
auditing, 1-5
authentication, 1-5

B

bidirectional traffic, 2-7

C

capi.exe file, 2-11
cipher algorithm, A-4
cipher block chaining, 2-10
cipher key, 3-2
confidentiality, 1-5
Configuration Manager, 3-6

D

DES, 1-4, 2-9
dial services, 1-2

E

educational services, xvii
encryption, 2-9, 3-1
ESP, 1-4, 2-7

F

frame relay, 1-2

H

HMAC MD5, 1-4, 2-10, A-5

I

IANA, 2-4
IETF, 1-1
Image Builder, 2-11
installation, 2-11
integrity, 2-10
Internet Protocol, 1-1
IP destination address, 2-6
IP interface, 1-1
IP Security, 1-1, A-2
IP source address, 2-8

K

k commands, 3-4, B-1

L

log, 3-6, 3-8

M

MD5, A-5
MIB, 3-2, 3-5

N

NPK, 3-2, A-1
NVRAM, 3-5, A-1

P

password, 3-4
policy template, 2-3, 3-7, 3-9
PPP, 1-2
product support, xvii
protocol, 1-2, 2-4
public data network, 1-3
publications, Bay Networks, xvi

R

random number, generating, 3-3
RNG, 3-2
router, 1-2
routers, supported, 1-2

S

SAD, 2-7
secure shell, 3-4
security association, 3-11
  protect, 2-4, 2-5, 3-12
  Site Manager parameters, A-3
  unprotect, 2-4, 3-11
security gateway, 2-3, 2-9
security parameter index (SPI), 2-6, 2-7, A-2
security policy
  action, 2-4, 2-5, 3-7, C-1
  criteria, 2-3, 2-4, 3-7
  examples, C-1
  inbound, 1-5, 2-3, 2-5
  outbound, 1-5, 2-3, 2-5, 3-9, A-2
  Site Manager parameters, A-2
security policy database (SPD), 2-6
seed for encryption, generating, 3-4
Site Manager, 1-1, 3-6, A-1
subnetwork, 2-2
support, Bay Networks, xvii

T

technical publications, xvi
technical support, xvii
Technician Interface, 3-3, 3-4
text conventions, xiv
tunnel mode, 1-3

V

VPN, 1-1

W

WAN, 1-2, 2-2, 3-8
WEP Key Manager, 3-3